

ABSTRACT

A Certificate Status Service that is configurable, directed, and able to retrieve status from any approved Certification Authority (CA) is disclosed. The CSS may be used by a Trusted Custodial Utility (TCU) and comparable systems or applications whose roles are validating the right of an individual to perform a requisite action, the authenticity of submitted electronic information objects, and the status of authentication certificates used in digital signature verification and user authentication processes. The validity check on authentication certificates is performed by querying an issuing CA. Traditionally, to create a trusted Public Key Infrastructure (PKI) needed to validate certificates, complex relationships are formed by cross-certification among CAs or by use of PKI bridges. The PKI and CA interoperability problem is addressed from a different point of view, with a focus on establishing a trust environment suitable for the creation, execution, maintenance, transfer, retrieval and destruction of electronic original information objects that may also be transferable records (ownership may change hands). A TCU is concerned only with a known set of "approved CAs" although they may support a multitude of business environments, and within that set of CAs, only with those certificates that are associated with TCU user accounts. Building PKI/CA trusted relationships is not required as the CSS achieves a trusted environment by querying only approved CAs and maintaining caches of valid certificates' status.